

IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF PUERTO RICO

NAICOM CORPORATION; D&V IP HOLDINGS,  
LLC; PAYLINK, LLC; AND  
Kiaras, LLC

PLAINTIFF,

v.

DISH NETWORK CORPORATION; DISH NETWORK,  
LLC; NAGRATAR, LLC; BERT EICHHORN,  
NAGRATAR INVESTIGATOR; EMILY RINKLE,  
NAGRATAR INVESTIGATOR; JORDAN SMITH,  
NAGRATAR INVESTIGATOR; KEVIN GEDEON,  
DISH NETWORK INVESTIGATOR; BRIAN PARSON;  
DISH NETWORK COLLABORATOR; THE UNITED  
STATES ATTORNEY OFFICE FOR THE DISTRICT OF  
PUERTO RICO; ROSA EMILIA RODRIGUEZ-VELEZ,  
FORMER UNITED STATES ATTORNEY; JOSE CAPO-  
IRRIARTE, FORMER AUSA, CHIEF CRIMINAL  
DIVISION; NICHOLAS W. CANNON, AUSA,  
DEPUTY CHIEF, CYBERCRIMES, CRIMINAL  
DIVISION; THE FEDERAL BUREAU OF  
INVESTIGATION, SAN JUAN, FIELD, IN PUERTO  
RICO; DOUGLAS A. LEFF, FBI SPECIAL AGENT IN  
CHARGE OF SAN JUAN DIVISION; BRADLEY REX,  
FBI SUPERVISORY SPECIAL AGENT; LANCE  
LANGE, FBI SPECIAL AGENT; KEVIN REAVES, FBI  
SPECIAL AGENT; CLAY REHRIG, FBI SPECIAL  
AGENT; JUAN GALARZA, FBI COMPUTER  
SCIENTIST; JASON LOPEZ, FBI EVIDENCE  
TECHNICIAN; SEVERAL UNKNOWN NAMES  
AGENTS OF FEDERAL BUREAU OF  
INVESTIGATIONS; JOHN DOES 1-20.

DEFENDANTS.

Civil Action No. 21-1405

COMPLAINT

JURY TRIAL DEMANDED

COUNT ONE

RICO (18 U.S.C. § 1962(c))

COUNT TWO

RICO CONSPIRACY (18 U.S.C. §  
1962(d))

COUNT THREE

COMPUTER FRAUD AND ABUSE  
ACT (18 U.S.C. § 1030(a))

COUNT FOUR

STORED COMMUNICATIONS ACT  
(18 U.S.C. §§ 2701-12)

COUNT FIVE

DIGITAL MILLENNIUM  
COPYRIGHT ACT (17 U.S.C. § 1201 et  
seq.)

COUNT SIX

MISAPPROPRIATION OF TRADE  
SECRETS UNDER THE DEFEND  
TRADE SECRETS ACT (18 U.S.C. §  
1836 et seq.)

COUNT SEVEN

PUERTO RICO INDUSTRIAL AND  
TRADE SECRETS PROTECTION ACT  
(Law No. 80, of June 3, 2011).

**COMPLAINT**

**TO THE HONORABLE COURT:**

Plaintiffs, **D&V IP HOLDINGS, LLC; NAICOM CORPORATION; KIARAS, LLC, PAYLINK, LLC**; through their undersigned counsel, most respectfully pray and request:

**NATURE OF ACTION**

**I. INTRODUCTION**

1. The tree of law must be pruned from time to time so that its branches keep our government institutions lawful. Our founders delegated this duty to the judiciary branch; no one is above the law.
2. Darwin Quinones-Pimentel (“Darwin”) is a veteran in systems architect with expertise in coding, algorithms and methods, software designs, formulas, patterns, compilations, programs, device methods, UI designs, database designs, network architect, and successful project leader with many other extraordinary skills in the computer science technology industry.
3. Beginning in the year 2002 through 2012, Darwin invested 10 years, a great expense of personal monetary funds, an extraordinary effort in developing a new distribution technology system to transmit live television programming content to residential and business customers using Multicast system via private Networks and the Internet.

4. Darwin's source codes and algorithms methods allow the passing of multicast traffic through networks no matter how the routers were configured by ISP companies, thus, the most efficient way of live TV distribution, a technology concept never known or used, because the Cable and Satellite TV industry did not have the solution to pass this type of traffic via the internet to end users, using server equipment, and filtering multicast content through tunnels by delivering only what the receiver is viewing.
5. Darwin's proprietary solution also managed to transcode the video and audio traffic to 2mps maintaining a broadcast quality in Full HD. A technology feature that the Cable and Satellite TV companies could not execute since their current distribution technology required at least more than 10mps to maintain the same quality and the TV content distributors had to transmit all the channels at the same time even though the receiver could only watch one. One good example is that when cable tv companies were transmitting 120 channels at the same time, the transmission required 1200mps to be able to deliver the 120 channels. On the other hand, Darwin's technology allowed the distribution of 200 channels and the end user only needs 2mps.
6. This proprietary solution enabled for the first time the broadcast of media via private networks and the internet, a new concept of IPTV service to distribute Live-Video Television Content (media) to residences, business, and primes customers.

7. Darwin's proprietary solution was characterized under the concept of Dynamic Internet Semantic Multicast Environment ("DISME"), a new technology concept that was not known in the Cable, Satellite, or IPTV industry, and unascertainable by any means, since according to engineer's expert in the computer science and telecommunications industry, claimed that the DISME concept, of distributing live television content using Multicast system via the Internet was impossible.
8. The DISME proprietary code sources were kept secret and confidential and were never revealed to any person, employee, company, corporation or third party, protected in a Hard Drive secured in a Safe Box and guarded under the protections of the Federal Defend Trade Secrets Act ("DTSA") (18 U.S.C. § 1836).
9. On April 9, 2012, the Federal Communications Commission (FCC), issued its Second Report of the Video Programming Accessibility on the Twenty-First Century Act of 2010, recognizing and encouraging the implementation of distribution of Digital Broadcast Television using Internet Protocol Television (IPTV) for customers in the United States.
10. In 2016, the DISME Technology was fully developed, and all alfa/beta tests were completed. Darwin and Victor Vega Encarnacion ("Mr. Vega" or collectively "Naicom's Founders) created Naicom Corporation, a Network & Internet Communication Platform capable of delivering live Television, Video on Demand

content via private fiber, internet and wireless network to subscribers worldwide, instant access to their favorite TV Shows, Movies, Music/Videos on Demand and Live Sports & Music events through its Set-Top-Box using the Internet Protocol Television and TV Everywhere (TVE) on any mobile device.

11. During this same period Darwin and Mr. Vega also engaged in joint business ventures marketing Kiaras, LLC a Human Resources, Time and Attendance Management company, and PayLink, LLC, a Payroll Processing company which confidential information and programs were filed, stored, secured in Naicom's Offices computers and filing cabinets. Paylink, LLC source codes were copyrighted and filed with the U.S. Copyright Office.

## **II. OVERVIEW OF THE CONSPIRACY**

12. From 2017 through 2019, the United States Attorney's Office for the District of Puerto Rico, through the coordinated efforts of the defendants, former U.S. Attorney for the District of P.R. Rosa Emilia Rodriguez-Velez,AUSA Jose Capo-Irriarte, AUSA, Nicholas W. Canon and the Federal Bureau of Investigation, San Juan, Field Office, FBI S/A Douglas A. Leff, FBI S/A Bradley Rex, FBI S/A Lance Lange, FBI S/A Kevin Reaves, FBI S/A , FBI S/A Clay Rehrig, FBI S/A Juan Galarza, FBI S/A Jason Lopez, ("collectively the Federal Defendants"), Dish Network Corporation, Dish Network, LLC Nagrastar, LLC, and NagraStar and Dish Network investigators Bert Eichhorn, Emily Rinkle, Jordan Smith,

Kevin Gedeon, and John Does 1-20 (collectively “the Dish Network defendants”), formed an association in fact racketeering enterprise through the power of their respective Enterprises and Legal Entities to deprive Plaintiffs of their Intellectual Property, Trade Secrets, and destroy their companies.

13. In order to accomplish the racketeering scheme and the conspiracies illegal objectives, the Dish Network and Federal defendants invented a criminal hoax against Naicom’s founders to secure an unlawful search warrant to facilitate the Dish Network defendants (Naicom’s competitors) access to enter Plaintiff’s private companies’ offices and data center and allow the Dish Network defendants access to misappropriate themselves of Plaintiffs’ Intellectual Property and Trade Secrets.
14. On August 27, 2019, the Federal defendants applied for two Search and Seizure Warrants; (1) Case No. 19-1680 (SCC), to search the premises of Building Centro de Seguro’s, 701 Ponce de Leon, Suite 208, San Juan, Puerto Rico 00907; and (2) Case No. 19-1679 (SCC), to search the premises of Villa Fontana, 4SS N2 Via Josefina, Carolina, PR.
15. The Federal defendants secured the above-mentioned search warrants under unlawful means using an affidavit in support of probable cause containing information known to be false and perjured in violation the United States criminal laws as prohibited pursuant to 18 U.S.C.A. § 2235- Search warrant

procured maliciously: 18 U.S.C.A. § 1621- Perjury generally, 18 U.S.C.A. § 1001- False Statements or entries generally.

16. On August 27, 2019, the FBI executed the search warrant and seized Documents, 2 Hard Drives, 2 USB Thumb Drives, 1 Cell Phone and 1 Tablet from Naicom Corporation, Naicom Data Center, Artist Designs and Management Corporation Offices, containing confidential information.
17. During the unlawful and warrantless search, the Federal defendants allowed the Dish Network defendants to enter and search Naicom's premises under the pretense that they were federal agents in violation of 18 U.S.C.A. § 912- Officer or employee of the United States; while exceeding the scope of the search warrant, thus, committing a warrantless search in a private company (Artist Designs and Management Corporation), and a second one in Naicom's Data Center in violation of 18 U.S.C.A. § 2234-Authority exceeded in executing warrant; 18 U.S.C.A. § 2236- Searches without warrant; and also disclosed and allowed the Dish Network defendants to learn about the confidential information in further violation of 18 U.S.C.A. § 1905- Disclosure of Confidential Information.
18. The underlying basis for the search warrant was false and the search warrant against plaintiffs' was dismissed on the government's own motion on 11/05/2019, Dkt 13, ("ORDER re 12 Notice (Other), re 10 Report and Recommendation, re 1 Motion for Return of Property: NOTED. Claimant

having waived the 14-day period to file objections to the Report and Recommendation (R&R), the Court ADOPTS the R&R and *orders the government to return the property listed in claimant's demand.* (Docket No. 1)" pursuant to Rule 41 of the Federal Rules of Criminal Procedure.

19. The Dish Network and Federal defendants' criminal investigation was nothing more than a ruse to attempt to deprive Plaintiffs of their Intellectual Property and Trade Secrets through a pattern of racketeering activities as prohibited under Mail Fraud (18 U.S.C. § 1341); Wire Fraud (18 U.S.C. § 1343); Conspiracy to Commit Mail And Wire Fraud (18 U.S.C. § 1341); Misappropriation Of Trade Secrets Under The Defend Trade Secrets Act (18 U.S.C. § 1836 et seq.); and the Puerto Rico Industrial And Trade Secrets Protection Act (Law No. 80, of June 3, 2011).
20. During the period of the criminal investigation, execution of the unlawful and warrantless searches and seizures, the Dish Network and Federal defendants illegally searched and gained access to Naicom's Offices and Data Center computers, servers, hardware equipment containing D&V IP Holdings, Naicom Corporations, Kiaras, LLC and Paylink, LLC, confidential information, intellectual property, trade secrets, and copyrighted computer programs in violation of the Computer Fraud and Abuse Act (18 U.S.C. § 1030(a)); Stored Communications Act (18 U.S.C. §§ 2701-12); and Digital Millennium Copyright Act (17 U.S.C. § 1201 et seq.).

21. Plaintiffs bring this action to address the individual and collective unlawful conduct of the Dish Network and Federal defendants under the statutes and common law discussed herein and are entitled to redress and relief from all those involved in the scheme to deprive Plaintiffs of their intellectual property and trade secrets.

**JURISDICTION AND VENUE**

22. This Court has federal question jurisdiction pursuant to 28 U.S.C. § 1331 because this action arises under 18 U.S.C. § 1030 (the Computer Fraud and Abuse Act); 18 U.S.C. §§ 1961-68 (Racketeer Influenced and Corrupt Organizations Act); 18 U.S.C. §§ 2701-11 (the Stored Communications Act); The Defend Trade Secrets Act of 2016, codified at 18 U.S.C. § 1836; Original jurisdiction is granted to the federal courts by 18 U.S.C. 1836(c); and 17 U.S.C. § 1201 et seq. (the Digital Millennium Copyright Act), and 17 U.S.C. § 1203, Civil Remedies.
23. This Court has supplemental jurisdiction over the state law claims alleged in this action, pursuant to 28 U.S.C. § 1337(a), because these claims are so intimately related to claims in the action exclusively within the Court's original jurisdiction that they form part of the same case or controversy under Article III of the United States Constitution, and because these claims arise out of the same nexus of facts and events. In addition, this Court has jurisdiction over this case pursuant to 28 U.S.C. § 1332(a)(2), because this suit is between a citizen of a domestic state (NAICOM CORPORATION), and a citizen of a foreign state (DISH NETWORK

CORPORATION) and the amount in controversy exceeds \$75,000; and section 1343 (1)(3)(4), pendent jurisdiction to hear and decide claims arising under state law.

24. Plaintiffs further invoke the supplemental jurisdiction of this Court to hear and adjudicate claims arising under the laws of the Commonwealth of Puerto Rico, specifically, Puerto Rico Industrial and Trade Secrets Protection Act (Law No. 80, of June 3, 2011), since they are so related to the federal claims that they all form part of the same case or controversy under Article III of the Constitution of the United States.
25. Venue is proper in this Court under 28 U.S.C. § 1391(b)(2) because these causes of action arose out of several incidents/events occurring in the Commonwealth of Puerto Rico, in the Jurisdiction of the United States District Court of Puerto Rico. Venue is also invoked pursuant to 28 U.S.C. § 1391(e)(1) since many of the defendants in this civil action are employees of the United States and were acting under color of legal authority when the constitutional cause of action accrued and a substantial part of the events or omissions giving rise to the claim occurred.
26. Venue is also proper for the claims arising under RICO pursuant to 18 U.S.C. § 1965(a) because some of the defendants reside, are found, have agents, or transacts his affairs, Dish Network Corporation, does business, as Dish Network, PR, in San Juan, Puerto Rico.

#### **PARTIES AND PARTICIPANTS**

27. Naicom Corporation was organized in 2016 as a corporation existing under the laws

of the Commonwealth of Puerto Rico with its place of business located at Building Centro de Seguros, 701 Ponce de Leon, Suite 208, San Juan, Puerto Rico 00907.

28. D&V IP HOLDINGS, LLC was organized in 2016 as a corporation existing under the laws of the Commonwealth of Puerto Rico with its place of business located at Building Centro de Seguros, 701 Ponce de Leon, Suite 208, San Juan, Puerto Rico 00907.
29. Paylink, LLC was organized in 2014 as a corporation existing under the laws of the Commonwealth of Puerto Rico with its place of business located at Building Centro de Seguros, 701 Ponce de Leon, Suite 208, San Juan, Puerto Rico 00907.
30. Kiaras, LLC was organized in 2010 as a corporation existing under the laws of the Commonwealth of Puerto Rico with its place of business located at Building Centro de Seguros, 701 Ponce de Leon, Suite 208, San Juan, Puerto Rico 00907.
31. Defendant, DISH Network Corporation, was organized in 1995 as a corporation under the laws of the State of Nevada. Dish Network started offering the DISH® branded pay-tv service in March 1996 and are the nation's third largest pay-tv provider. Dish Network's principal executive offices are located at 9601 South Meridian Boulevard, Englewood, Colorado 80112; telephone number (303) 723-1000.
32. Defendant, NagraStar, LLC 90 Inverness Cir E, Englewood, CO 80112 is a joint venture between Dish Network Corporation (formerly EchoStar Communications Corporation) and Kudelski SA that was formed in 1998. NagraStar's main focus is

delivering and maintaining security solutions for satellite and Internet-based television systems and other connectivity initiatives in North America. Their mission also includes carrying strong anti-piracy activities from field investigations to legal and joint actions with law enforcement agencies. The company is located onsite with Dish in Colorado. NagraStar is a joint venture between Dish Network Corporation (formerly EchoStar Communications Corporation) and Kudelski SA that was formed in 1998.

33. Defendant Jordan Smith is and was at all times relevant herein a resident of Parker, Colorado, employed by NagraStar as Manager of Field Security Investigations and Senior Anti-Piracy Investigator. Defendant Jordan Smith participated individually and collectively in concert with the above-captioned defendants in the violation of the above statutory criminal and civil offenses.
34. Defendant, Bert Eichhorn is and was at all times relevant herein a resident of Denver, Colorado, employed by NagraStar as Manager of Field Security & Investigations. Defendant Bert Eichhorn participated individually and collectively in concert with the above-mentioned defendants in the violation of the above statutory criminal and civil offenses.
35. Emily Rinkle is and was at all times relevant herein, a resident of Denver, Colorado, employed by NagraStar as the Manager of Field Security & Investigations. Defendant Emily Rinkle participated individually and collectively in concert with

the above-captioned defendants in the violation of the above statutory criminal and civil offenses.

36. Defendant, Kevin Gedeon, is and was at all times relevant herein, a resident of Lone Tree, Colorado, employed by Dish Network as the Manager of Fraud Investigations. Defendant Kevin Gedeon participated individually and collectively in concert with the above-captioned defendants in the violation of the above statutory criminal and civil offenses.
37. Upon information and belief, Defendant, Brian Parsons, is and was at all times relevant herein, a resident of Saint Peters, Florida, either employed or collaborator with Dish Network defendants, Managers of Fraud Investigations division. Defendant Brian Parsons participated individually and collectively in concert with the above-captioned defendants in the violation of the above statutory criminal and civil offenses.
38. Defendant Rosa Emilia Rodriguez-Velez was at all times relevant herein, a resident of Puerto Rico, employed by the United States Government. Rosa Emilia Rodriguez-Velez was appointed by the District Court to serve as the United States Attorney for the District of Puerto Rico, until the vacancy was filled, and charged with the duties to investigate, collect, analyze, and corroborate evidence in support of search warrant probable cause determinations and prosecutions in violation of the laws against the United States in the Criminal Division of the District of Puerto Rico. She

was sworn under oath before taking office to execute faithfully her duties, the United States Laws, uphold Local Laws, and to abide by the United States Constitution. Defendant Rosa Emilia Rodriguez-Velez participated individually and collectively in concert with the above-captioned defendants in the violation of the above statutory criminal and civil offenses.

39. Jose Capo-Irriarte was at all times relevant herein, a resident of Puerto Rico, employed by the United States Government. Jose Capo-Irriarte was appointed by the Attorney General as Assistant United States Attorney, in the District of P.R., to assist the United States Attorney as the Chief of the Criminal Division and charged with the duties to investigate, collect, analyze, and corroborate evidence in support of search warrant probable cause determinations and prosecutions in violation of the laws against the United States in the Criminal Division of the District of Puerto Rico. He was sworn under oath before taking office to execute faithfully his duties, the United States Laws, uphold Local Laws, and to abide by the United States Constitution. Defendant Jose Capo-Irriarte participated individually and collectively in concert with the above-captioned defendants in the violation of the above statutory criminal and civil offenses.
40. Nicholas W. Cannon is and was at all times relevant herein, a resident of Puerto Rico, employed by the United States Government as Assistant United States Attorney, Deputy Chief, Cybercrimes, Criminal Division in the District of P.R. As Assistant United States Attorney, Nicholas W. Cannon was appointed by the

Attorney General to assist the United States Attorney for the District of Puerto Rico, and charged with the duties to investigate, collect, analyze, and corroborate evidence in support of search warrant probable cause determinations and prosecutions in violation of the laws against the United States in the Criminal Division of the District of Puerto Rico. He was sworn under oath before taking office to execute faithfully his duties, the United States Laws, uphold Local Laws, and to abide by the United States Constitution. Defendant Nicholas W. Cannon participated individually and collectively in concert with the above-captioned defendants in the violation of the above statutory criminal and civil offenses.

41. Defendant Douglas A. Leff was at all times relevant herein, a resident of Puerto Rico, and the FBI Special Agent in Charge of the San Juan Division. As FBI Special Agent in Charge of the San Juan Division, Douglas A. Leff was responsible for overseeing and supervising all criminal investigations conducted by the FBI San Juan Division. FBI Special Agent Douglas A. Leff was also charged with the duty and power to enforce the criminal laws of the United States, to execute and serve search warrants, arrest warrants, and to make seizures of property. Douglas A. Leff was also responsible for reviewing, analyzing, and discussing with the FBI Legal Counsel if the evidence collected during criminal investigations by his FBI Agents subordinates qualified as evidence supporting probable cause pursuant to Fourth Amendment constitutional standards in support of search warrant applications for criminal prosecutions in the District of Puerto Rico. He was sworn under Oath to

faithfully execute the laws of the United States, uphold local laws and to abide by the United States Constitution. The defendant Douglas A. Leff participated individually and collectively in concert with the above-captioned defendants in the violation of the above statutory criminal and civil offenses.

42. Defendant Brad Rex is and was at all times relevant herein, a resident of Puerto Rico, and the FBI Supervisory Special Agent in the San Juan Division. As the FBI Supervisory Special Agent in the San Juan Division Brad Rex was charged with the responsibility of supervising and assuring that the FBI Special Agents assigned to his squad would follow the rule of law. FBI Special Agent Brad Rex was also charged with the duty and powers to enforce the criminal laws of the United States, to execute and serve search warrants, arrest warrants and to make seizures of property. FBI Special Agent Brad Rex was also responsible for reviewing, analyzing, and discussing with the FBI Legal Counsel if the evidence collected during criminal investigations by his FBI Agents subordinates qualified as evidence supporting probable cause under Fourth amendment constitutional standards in support of search warrant applications for criminal prosecution in the District of Puerto Rico. He was sworn under Oath to faithfully execute the United States Laws, uphold local laws and to abide by the United States Constitution. The defendant Brad Rex participated individually and collectively in concert with the above-captioned defendants in the violation of the above statutory criminal and civil offenses.

43. Defendant Lance Lange is and was at all times relevant herein a resident of Puerto Rico and Special Agent in the San Juan Division. As Special Agent in the San Juan Division Lance Lange was charged with the duty and powers to enforce the criminal laws of the United States, to execute and serve search warrants, arrest warrants, and to make seizures of property. As such he was sworn under oath to faithfully execute the United States Laws, uphold the local laws and to abide by the United States Constitution. The defendant Lance Lange participated individually and collectively in concert with the above-captioned defendants in the violation of the above statutory criminal and civil offenses.
44. Defendant Kevin Pearson is and was at all times relevant herein, a resident of Puerto Rico, and Special Agent in the San Juan Division. As Special Agent in the San Juan Division Kevin Pearson was charged with the duty and powers to enforce the criminal laws of the United States, to execute and serve search warrants, arrest warrants, and to make seizures of property. He was sworn under Oath to faithfully execute the United States Laws, uphold the local laws and to abide the United States Constitution. The defendant Pearson participated individually and collectively in concert with the above-captioned defendants in the violation of the above statutory criminal and civil offenses.
45. Defendant Clay Rehrig is and was at all times relevant herein, a resident of Puerto Rico, and Special Agent in the San Juan Division. As Special Agent in the San Juan Division Clay Rehrig was charged with the duty and powers to enforce the criminal

laws of the United States, to execute and serve search warrants, arrest warrants, and to make seizures of property. He was sworn under oath to faithfully execute the United States Laws, uphold local laws and to abide by the United States Constitution. The defendant Clay Rehrig participated individually and collectively in concert with the above-captioned defendants in the violation of the above statutory criminal and civil offenses.

46. Defendant Juan Galarza is and was at all times relevant herein, a resident of Puerto Rico, and the FBI Computer Science Officer in the San Juan Division. As Computer Science Officer in the San Juan Division Juan Galarza was charged with the duty and powers to enforce the criminal laws of the United States, to execute and serve search warrants, arrest warrants, and to make seizures of property. He was sworn under oath to faithfully execute the United States Laws, uphold local laws and to abide by the United States Constitution. Defendant Juan Galarza participated individually and collectively in concert with the above-captioned defendants in the violation of the above statutory criminal and civil offenses.
47. Defendant Jason Lopez is and was at all times relevant herein, a resident of Puerto Rico, and the FBI Evidence Technician in the San Juan Division. As FBI Evidence Technician in the San Juan Division Jason Lopez was charged with the duty and powers to enforce the criminal laws of the United States, to execute and serve search warrants, arrest warrants and to make seizures of property. He was sworn under Oath to faithfully execute the United States Laws, uphold local laws and to abide

by the United States Constitution. The defendant Jason Lopez participated individually and collectively in concert with the above-captioned defendants in the violation of the above statutory criminal and civil offenses.

48. Several Unknown Named Agents of Federal Bureau of Investigations also participated individually and collectively participated in concert with the above-captioned defendants in the violation of the above statutory criminal and civil offenses.
49. John Doe 1-20, individually and collectively participated in concert with the above-captioned defendants in the violation of the above statutory criminal and civil offenses.

**Other Relevant Persons and Legal Entities**

50. The United States Attorney Office for the District of Puerto Rico, is and was responsible for investigating, collecting, analyzing, and corroborating evidence in support of search warrant probable cause determination, the enforcement and prosecutions for violation of the laws against the United States in the Criminal Division of the District of Puerto Rico. Defendants Rosa Emilia Rodriguez-Velez former U.S. Attorney for the district of P.R., AUSA Jose Capo-Irriarte, AUSA and Nicholas W. Cannon used the power of the United States Attorney Office to advance the conspiratorial criminal/statutory violation objectives with the above-mentioned defendants, an association engaged in criminal enterprise racketeering activities.

51. The Federal Bureau of Investigation, San Juan, Field, in Puerto Rico, was responsible for investigating, detecting, and prosecuting crimes against the United States; and conducting such other investigations regarding official matters under the control of the Department of Justice and the Department of State as may be directed by the Attorney General. The defendants FBI S/A Douglas A. Leff, FBI S/A Bradley Rex, FBI S/A Lance Lange, FBI S/A Kevin Reaves, FBI S/A Clay Rehrig, FBI S/A Juan Galarza, FBI S/A Jason Lopez, used the power of the Federal Bureau of Investigation, San Juan, Field Office, to advance the conspiratorial criminal/statutory violation objectives in concert with the above-mentioned defendants an association engaged in criminal enterprise racketeering activities.

#### FACTUAL ALLEGATIONS<sup>1</sup>

### **III. D&V IP HOLDINGS AND NAICOM'S GENESIS**

52. Through the years 2015-2016, Darwin and Mr. Vega engaged in a joint business venture to create a Network and Internet Communications Company capable, among other matters, of offering IPTV services. In order to accomplish the business structure legal entity Darwin and Mr. Vega created two corporations, D&V IP Holding, LLC the company who would hold the DISME proprietary

---

<sup>1</sup> Please take Judicial notice that the record containing some of the evidence supporting factual allegations in this Civil Case are found in the Motion for Demand For Return of Property in the form of Attachments 1through 33 filed in miscellaneous Case No.[19-mc-308 (FAB)]. See Federal Rules of Civil Procedure Rule 10 Form of Pleadings (c) Adoption by Reference; Exhibits. A statement in a pleading may be adopted by reference elsewhere in the same pleading or in any other pleading or motion. A copy of a written instrument that is an exhibit to a pleading is a part of the pleading for all purposes. Id.

solution, source codes, technology, and Naicom Corporation, who would license the DISME technology from D&V IP Holding, LLC to use its technology to distribute television programing from authorized content providers networks.

53. In complementing the development of the DISME technology through the performance of alpha/ beta tests, D&V IP Holdings and Naicom Corporation, with considerable economic investment, created and developed significant amounts of confidential and proprietary information, including non-public information relating to DISME's source codes, algorithms and methods, technological vision for Naicom's IPTV content distribution, marketing and servicing; research and development efforts and strategies; business and marketing performance strategies; financial data and business plans; technical data; customer development; and subcontractor and vendor relationships. The same procedures were implemented for Kiara's and Paylink's corporations. (collectively, "Confidential Information").

54. In protecting and keeping the Confidential Information secret, D&V IP Holdings and Naicom Corporations, only installed on their servers, located at the Naicom's Data Center, what is known as a compiled executable. The entire system was installed with Ubuntu operating system which allows the hard disk to be encrypted. To access Naicom's servers the authorized employee needed to enter a secure data center building structure, and access its computer systems

through user and password, which were assigned by hierarchy. The SSH access is in private LAN, which is not exposed to the internet, to be able to attack the server through internal ports it was necessary to be inside the building. The same procedures were implemented for Kiara's and Paylink's corporations.

55. In 2016, Darwin and Victor founded and registered in the State Department of Puerto Rico Naicom Corporation as a closed corporation business company doing business in Puerto Rico and complied with all the requirements to perform as a legitimate IPTV business.
56. In 2016, Naicom Corporation also requested the manufacture of its own brand of tv set top boxes for end users through Informir LLC. The communication between Naicom's TV Set Top Box and the servers also had what is known as a security hash and key.
57. In 2016, Naicom Corporation acquired the programing licenses to distribute television media and video on demand content in United States, Puerto Rico and U.S. Virgin Islands through worldwide television network companies and in 2017, Naicom Corporation became a member of the National Rural Telecommunications Cooperative "NRTC".
58. In 2016, Naicom Corporation began exploring the search of potential business negotiations with other cable tv companies and executed Naicom's Business

Executive Summary and Valuation for potential Investors.

59. On January 6, 2017, Naicom Corporation submitted a request to have Apple Corporation place its Naicom TV App in Apple's AppStore. Apple Corporation's legal division requested Naicom Corporation to produce all the licenses authorizing the programming distribution available to Naicom's subscribers via Naicom TV TVE function at iPhone Cellular phones.
60. On February 16, 2017, Apple Corporation approved Naicom Corporation App for Apples' AppStore as Naicom TV App.
61. On December 15, 2017, Sams Club approved Naicom Corporation to officially launch and distribute in their retail stores the Naicom's IPTV Set Top Box which offered the distribution of tv programming to customers in Puerto Rico.
62. D&V IP Holdings, Naicom, Kiara and Paylink Corporations also developed policies and practices to maintain the secrecy of its confidential and proprietary information, including, internal policies and procedures regarding the identification and classification of proprietary and confidential information.
63. To safeguard D&V IP Holdings', Naicom's, Kiaras' and Paylink's own confidential information and proprietary data as well as that of customers and other third parties, the corporations restricts employees' access to confidential and proprietary information as required by each employee's business needs and

requires employees to execute non-disclosure agreements, among other protections.

64. D&V IP Holdings, Naicom, Kiaras and Paylink also invested significantly to acquire and implement multi-faceted layered data security technology and other protections in order to safeguard its confidential and proprietary data, including, for example: Imposing restrictions on remote access to corporations networks; Requiring individual password protection; Implementing data encryption on the corporations computers, servers, and Naicom's mobile devices TV application; and conducting internal periodic cybersecurity audits.
65. Pursuant to its internal policies, the classification "D&V IP Holdings, Naicom, Kiaras and Paylink Proprietary" applies to the corporation's internal and contractually protected highly sensitive information, where compromise would be substantially and irreversibly detrimental to the corporations business interests. D&V IP Holdings', Naicom's, Kiaras' and Paylink's internal policies regarding the safeguarding of corporations Proprietary Information specifically includes in the definition of "D&V IP Holdings', Naicom's, Kiaras' and Paylink's Proprietary and Confidential Information" all technical information, source codes, formulas, contracts data, systems designs, algorithms and methods, performance capabilities, data relating to Naicom's, Kiaras' and Paylink's business operations and administration, trade secrets, data protected by state or federal privacy regulations, proposal data, financial and employee

information, intellectual property, and data pertaining to D&V IP Holdings', Naicom's, Kiaras' and Paylink's technical developments.

66. D&V IP Holdings', Naicom's, Kiaras' and Paylink's policies require that documents containing D&V IP Holdings', Naicom's, Kiaras' and Paylink's Proprietary and Confidential Information shall be conspicuously marked with a legend identifying the document as "D&V IP Holdings', Naicom's, Kiaras' and Paylink's Proprietary" in accordance with internal operating guidelines for the marking, maintenance, and transmittal of proprietary information. Documents submitted to potential investors, content providers networks, companies and business were further marked "Confidential Information" in addition to bearing "D&V IP Holdings', Naicom's, Kiaras' and Paylink's Proprietary" markings.

#### **IV. THE NEGOTIATIONS WITH CLARO PUERTO RICO**

67. In 2017, CLARO Puerto Rico began negotiations with Naicom Corporation to distribute Naicom Set Top Boxes to their customers.
68. Claro represented to Naicom Corporation that it had approximately 320,000 internet subscribers that could not subscribe to Claro's IPTV services because Claro's internet distribution to those residences delivered only 5 Megabytes and Claro's IPTV Set Top Box required 60 Megabytes to adequately upload the Claro's IPTV distribution programing.

69. During the negotiation process Naicom Corporation and Claro Puerto Rico executed a mutual NDA agreement prior to having the executive members meeting to discuss and analyze business information involving the letter of intent and the resellers agreement contents.
70. After extensive business negotiations Claro's Product Development Officer Anibal Rios represented to Naicom executives that the Claro-Naicom business alliance represented to Claro business projections of over \$10,000,000 of monthly gross revenue for the first year and over \$13,000,000 for the second year just by penetrating Claro's corporate and residential subscribers in Puerto Rico.
71. On the other hand, the Claro-Naicom business alliance represented to Naicom business projections to achieve 100,000 Corporate subscribers, plus another 150,000 residential subscribers, projecting a monthly income revenue of \$9,000,000 in the first year, and \$12,000,000 for the second year in gross sales to Claro's subscribers and Naicom's new customers.
72. Upon information and belief, Claro had a contract with Dish Network Satellite TV, where Dish Network was providing the TV programming to Claro's internet subscribers which could not subscribe to Claro's IPTV services and the Naicom deal represented a contract cancelation threat to Dish Network's contract with Claro, and Claro was also considering shutting down its IPTV business division for loss of revenue.
73. Mr. Carlos Garcia of Claro Puerto Rico assisted to several meetings during the

Claro-Naicom deal negotiations since he was Claro's IPTV business Manager. During these meetings Mr. Carlos Garcia became privy to the details of the Claro-Naicom deal would leave him jobless if Claro opted at the end to shut down the IPTV division he managed.

74. Upon information and belief Mr. Carlos Garcia fears moved him to alert the executives of Dish Network Puerto Rico that Claro-Naicom's IPTV deal would require the cancelation of Dish Network Satellite TV contracts with Claro and even he could lose his job. The Naicom-Claro IPTV deal news caused Dish Network great animosity towards Naicom TV in the industry of Cable and IPTV market.
75. Upon information and belief, Mr. Carlos Garcia convened the Dish Network defendants and convinced them that Naicom TV was an IPTV pirate company because he had sent Claro's employees to photograph Naicom's Data Center and the way Naicom established its satellite dishes lock angle indicated that Naicom dishes were being used for TV piracy.
76. Naicom's Data Center employees caught Claro's employees photographing Naicom's Data Center and the photos and the issue was brought to Claro's Puerto Rico President Enrique Ortiz.
77. August 14, 2018, after a year of meetings, the Naicom-Claro IPTV negotiation was a done deal. Nevertheless, for reasons unbeknownst to Naicom Corporation's executive officers, Claro mysteriously disappeared from the table of negotiations and never informed Naicom Corporation why they pulled out of the deal.

78. Upon information and belief, the Dish Network defendants, informed Claro's executives to withdraw from the deal because the FBI was investigating Naicom and its founders for criminal prosecution.

**V. THE DISH NETWORK CORPORATION RACKETEERING ENTERPRISE.**

79. On August 7, 2017, the Dish Network defendants acting through its employees instructed Brian Parsons to purchase a Naicom TV Set Top Box receiver to spy and conduct reverse engineering tests on Naicom's IPTV Set Top Box middle firmware. Brian Parsons placed the order via Naicom's website, registered online the following information: BRIAN PARSONS, Phone (727) 409-9464, Email: [parsons.brian716@outlook.com](mailto:parsons.brian716@outlook.com) Address: 9079 FOURTHSTREET NORTH SAINTPETERS FL 33702 IP: 70.127.233.139, Created: 03/07/2018 03:01 PM Visa ending in 2775, and purchased two Naicom's IPTV set top boxes, MAC Numbers 00:1A:79:46:97:AD; and 00:1A:79:46:A4:BE which were mailed to Brian Parsons residence, via the United States Postal Service, to the above address.
80. According to Dish Network defendants acting through their employees the defendants Kevin Gedeon, Jordan Smith, Bert Eichhorn and Emily Rinkle, their investigation revealed that the receiver provided access to approximately 43-channels- including channels such as Disney, TBS, ESPN, CNN, HBO, Showtime, and Cinemax.

81. The Dish Network defendants acting through their employees' defendants Kevin Gedeon, Jordan Smith, Bert Eichhorn and Emily Rinkle investigators downloaded the Naicom TV application through Apples' Appstore, which required a registration to enable the subscriber to create its login credentials as the receiver and provided access to approximately 42 channels.
82. The Dish Network defendants acting through their employees, the defendants Kevin Gedeon, Jordan Smith, Bert Eichhorn and Emily Rinkle also tested Naicom TV several times to identify if it was providing DISH programming and in each case the test revealed no DISH content.
83. Upon information and belief, Dish Network defendants acting through their employees, the defendants Kevin Gedeon, Jordan Smith, Bert Eichhorn and Emily Rinkle also contacted several Media Companies<sup>2</sup> Content providers to inquire as to whether Naicom had the appropriate licensing contracts to distribute its programming and on each occasion these defendants were informed that Naicom Corporation was authorized to distribute its content.
84. Upon information and belief, Dish Network defendants acting through their employees, the defendants Kevin Gedeon, Jordan Smith, Bert Eichhorn and Emily Rinkle conducted reverse engineering through the use WireShark program on

---

<sup>2</sup> It should be noted that Dish Network was a member of the same content programming Network Media Companies that licensed Naicom the authorization to distribute television programming content.

Naicom's IPTV Set Top Box and discovered that Naicom's TV technology performed its tv programming distribution service to its end user with the use of only 2mps, and this was a threat to Dish Network and Sling TV to the future competition for subscribers in Puerto Rico and the United States.

**THE ULTRA VIRE MOTIVES BEHIND THE ALLEGED CRIMINAL INVESTIGATION.**

85. On March 18, 2019, Dish Network Company filed its ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934 with the UNITED STATES SECURITIES AND EXCHANGE COMMISSION, Washington, D.C. 20549 Form 10-K FOR THE FISCAL YEAR ENDED DECEMBER 31, 2018.
86. In said report Dish Network reported to its shareholders the risk companies like Naicom IPTV represented to their market as follows:
  - a. Changing consumer behavior and competition from digital media companies that provide or facilitate the delivery of video content via the Internet may reduce our subscriber activations and may cause our subscribers to purchase fewer services from us or to cancel our services altogether, resulting in less revenue to us.
  - b. Economic weakness and uncertainty may adversely affect our ability to grow or maintain our business.

- c. Our competitors may be able to leverage their relationships with programmers to reduce their programming costs and/or offer exclusive content that will place them at a competitive advantage to us.
- d. Our over-the-top (“OTT”) Sling TV Internet-based services face certain risks, including, among others, significant competition.
- e. If government regulations relating to the Internet change, we may need to alter the manner in which we conduct our Sling TV business, and/or incur greater operating expenses to comply with those regulations
- f. Technology in the pay-TV industry changes rapidly, and our success may depend in part on our timely introduction and implementation of, and effective investment in, new competitive products and services, and our failure to do so could cause our products and services to become obsolete and could negatively impact our business.
- g. Competition, our business has historically focused on providing pay-TV services. We face substantial competition from established pay-TV providers and broadband service providers and increasing competition from companies providing/facilitating the delivery of video content via the Internet to computers, televisions, and other streaming and mobile devices, including wireless service providers. In recent years, the traditional pay-TV industry has matured, and industry consolidation and convergence has created competitors

with greater scale and multiple product/service offerings.

- h. These developments, among others, have contributed to intense and increasing competition, and we expect such competition to continue.
- i. We also face increasing competition from content providers and other companies who distribute video directly to consumers over the Internet. These content providers and other companies, as well as traditional satellite television providers, cable companies and large telecommunication companies, are rapidly increasing their Internet-based video offerings. Programming offered over the Internet has become more prevalent and consumers are spending an increasing amount of time accessing video content via the Internet on their mobile devices. In particular, consumers have shown increased interest in viewing certain video programming in any place, at any time and/or on any broadband-connected device they choose. Video content distributed over the Internet includes services with live-linear television programming such as DirecTV Now, Sony PlayStation Vue, YouTube TV, Fubo TV, Philo TV and Pluto TV, as well as single programmer offerings such as HBO NOW, CBS All Access, STARZ and SHOWTIME and offerings of large libraries of on-demand content, including in certain cases original content, by companies such as Netflix, Hulu, Apple, Amazon, Alphabet and Verizon. Certain of these companies have invested extensive resources in producing original content that is exclusive to their

platform.

87. Upon information and belief, based on the above information, Dish Network defendants acting through their employees, the defendants Kevin Gedeon, Jordan Smith, Bert Eichhorn and Emily Rinkle filed a complaint with the Federal Bureau of Investigations falsely alleging that Naicom Corporation was running an IPTV pirate operation.
88. Upon information and belief, the true motive behind Dish Network defendants' complaint against Naicom was to secure a joint criminal investigation with the FBI, procure a search warrant, enter Naicom's Offices and Data Center premises to search/seize Naicom's computers, servers and other hardware containing the companies trade secrets and confidential information under the ruse of assisting the FBI in discovering incriminating evidence to appropriate themselves of D&V IP Holdings and Naicom's proprietary intellectual property, confidential information, and dismantle Naicom Corporation.
89. On August 27, 2019, the Federal Bureau of Investigations, acting through its employees FBI Special Agents Douglas A. Leff, Bradley Rex, Lance Lange, Kevin Reaves, Clay Rehrig, Juan Galarza, Several Unknown Names Agents Of Federal Bureau Of Investigations, facilitated the Dish Network defendants acting through their employees, the defendants Kevin Gedeon, Jordan Smith, Bert Eichhorn and Emily Rinkle (Naicom's competitors ) the authority to enter to Naicom's

Corporation Offices and Data Center under the ruse of a criminal investigation to execute unlawful search warrants and warrantless searches at its premises, and after shutting down Naicom IPTV distribution operations, the FBI allowed Dish Network and Nagrastar investigators to search its offices and data center computers, servers, hardware equipment, and photograph documents containing intellectual property, trade secrets, acquired intellectual property, trade secrets and confidential information, under the ruse that Darwin Quinones and Victor Vega were running an IPTV pirate operation through Naicom's Corporation.

90. Such Confidential Information is economically valuable to D&V IP Holdings' and Naicom's IPTV competitors and, as described previously, its value extends far beyond Dish Network's Sling TV streaming distribution technology. Dish Network defendants access to D&V IP Holdings' and Naicom's IPTV Confidential Information gives Dish Network defendants (and other D&V IP Holdings and Naicom's competitors) an unfair competitive advantage with respect to future commercial of television programming distribution. The bell cannot be unrung—Dish Network defendants cannot unlearn what they discovered and learned from D&V IP Holdings DISME technology and Naicom's Confidential Information it has now improperly accessed, and D&V IP Holdings and Naicom Corporation has no means, absent judicial intervention, of preventing Dish Network defendants from incorporating D&V IP HOLDINGS's DISME and Naicom's IPTV trade secrets, confidential and

proprietary information into Dish Network's own streaming technology, strategic plans and competing in the television programming distribution and public and private sector proposals contracts going forward.

VI.

**THE UNITED STATES ATTORNEY'S OFFICE AND FEDERAL BUREAU OF INVESTIGATIONS DEFENDANTS' INVOLVEMENT IN THE CONSPIRACY WITH THE DISH NETWORK DEFENDANTS TO DEPRIVE PLAINTIFFS OF THEIR INTELLECTUAL PROPERTY AND TRADE SECRETS.**

91. Upon information and belief, the United States Attorney's Office defendants, Rosa Emilia Rodriguez-Velez, AUSA Jose Capo-Irriarte, AUSA Nicholas W. Cannon and the Federal Bureau of Investigation defendants, FBI Special Agents Douglas A. Leff, Brad Rex, Kevin Reaves, Clay Rehrig, Juan Galarza, Jason Lopez, criminal investigation involvement with the Dish Network defendants acting through its employees, defendants Kevin Gedeon Jordan Smith, Bert Eichhorn and Emily Rinkle was nothing more than a criminal hoax scheme to facilitate the Dish Network defendants the authority to enter into Naicom's premises and give them access to misappropriate themselves from D&V IP Holdings and Naicom's Intellectual Property, Trade Secrets and confidential information, in violation of the United States RICO laws.
92. Upon information and belief, the Federal and Dish Network defendants accomplished the conspiracies objectives of the racketeering scheme by using the power of the United States Attorney Office and the power of the Federal Bureau of Investigation offices, to have them submit in Federal Court a sworn declaration

containing false/ perjured statements in support of a search warrant application to enter Naicom's premises when the Dish Network knew for a fact that the Federal defendants' investigatory files, logs, notes, memorandums, reports of investigation, photographs, videos, "the collected evidence," negated any criminal wrong doing that Naicom's founders were committing the crimes charged in the search and seizure warrant affidavit and application.

93. Upon information and belief, the Dish Network and Federal defendants also knew that Naicom Corporation in fact counted with the distribution licensing contracts of the following media networks Wapa TV, Disney, HBO, Turner, NBC, Condista, CBS, Telecinco, ABC, the National Rural Telecommunications Cooperative, and that Naicom Corporation was also authorized to market and sell its IPTV product through Apple Corporation, Walmart, Sams Club among other business associates.
94. On August 27, 2019, the defendants FBI S/A Brad Rex, Lance Lange, Kevin Reaves, Clay Rehrig, Juan Galarza, Jason Lopez, other FBI agents, agreed and in combination with the Dish Network defendants acting through its employees', defendants Kevin Gedeon, Jordan Smith, Bert Eichhorn and Emily Rinkle and posing as federal agents entered Naicom's Offices located at Building Centro de Seguros, 701 Ponce de Leon, Suite 207, San Juan, Puerto Rico 00907 and executed the unlawful search and seizure warrant.
95. During the execution of the search and seizure warrant the Dish Network

defendants acting through their employee defendant Bert Eichhorn who was posing as a federal agent appropriated himself of Naicom's Offices and Data Center keys belonging to Victor Vega and Darwin Quinones in the presence of defendant FBI S/A Lance Lange.

96. During the execution of the search and seizure warrant the Dish Network defendants acting through its employees' defendants Bert Eichhorn and Emily Rinkle also posing as federal agents entered Naicom's business office without the supervision of any FBI Agent, searched, inspected and photographed private documents containing business trade secrets, intellectual property and confidential information belonging to D&V IP Holdings, Naicom, Kiara, and Paylink corporations.
97. During the execution of the search and seizure warrants the Dish Network acting through its employees, defendants Bert Eichhorn and Emily Rinkle, also posing as federal agents, entered the office belonging to Victor Vega at Naicom premises without the supervision of any FBI Agent, searched, inspected and photographed private documents containing business trade secrets, intellectual property and confidential information belonging to the corporations.
98. During the execution of the search and seizure warrants the Dish Network defendants acting through its employee defendant Bert Eichhorn, also posing as a federal agent, was observed accessing Naicom's computers searching, reading,

photographing, downloading its contents which contained business trade secrets, intellectual property and confidential information belonging to the corporations.

99. In the aftermath of the execution of the search warrant Federal defendant Lance Lange in combination with the Dish Network defendants acting through its employees, defendants Bert Eichhorn and Emily Rinkle, also posing as federal agents, seized from the Plaintiffs, documents, 2 Hard Drives, 2 USB Thumb Drives, Cell Phone and 1 Tablet containing intellectual property, secret trade and confidential information belonging to the corporations.
100. On August 27, 2019, the Federal Bureau of Investigations, acting through its employees FBI Special Agents Kevin Pearson and several unknown agents of the FBI agreed and in combintion with the Dish Network defendants acting through its employees, defendants Jordan Smith and Kevin Gedeon, also posing as federal agents, entered Naicom Corporation's Data Center to execute a search and seizure warrant.
101. During the execution of the search and seizure warrant Darwin Quinones observed the defendant FBI S/A Kevin Pearson allowing the Dish Network defendants acting through its employees, the defendants Jordan Smith, and Kevin Gedeon who were posing as federal agents place a pen drive and connect cables to access, and perform a search into Naicom's Data Center Computers, Servers and other electronic Hardware containing intellectual property,trade secrets and confidential

information belonging strictly to the D&V IP Holding and Naicom corporations, and to take pictures of Naicom's Data Center structural/ network connections and collocation platform.

102. During the execution of the search and seizure warrant the Dish Network defendants acting through its employees, the defendants Jordan Smith, Kevin Gedeon who were posing as federal agents, interrogated Darwin Quinones and Naicom's employee Jaime Echevarria regarding the technology which distributed the programming, its functions and protocols.
103. At the conclusion of the search and seizure defendant AUSA Nicholas W. Cannon requested defendant FBI S/A Kevin Reaves to instruct Darwin Quinones and Victor Vega to report to the FBI Offices in San Juan with the licensing contracts for an interview regarding Naicom's company.
104. At the San Juan FBI offices defendant FBI S/A Kevin Pearson, and the Dish Network defendants acting through its employees, defendants Jordan Smith and Kevin Gedeon while posing as federal agents questioned Darwin Quinones in the presence of Naicom's legal Attorney Patricia Rivera as to how Naicom acquired the IPTV distribution contracts with the content providers and the technology to distribute the programming via private networks and the internet, inspected Naicom's contracts with the Networks Content Providers, containing trade and

busines secrets and confidential information justifying D&V IP Holdings DISME technology content programming distribution contracts belonging strictly to Naicom Corporation.

VII. **THE UNLAWFUL TRESPASSING INTO NAICOM'S DATA CENTER'S PRIVATE PROPERTY TO REATTEMPT TO MISAPPROPRIATE THEMSELVES WITH D&V IP HOLDINGS AND NAICOM CORPORATIONS TRADE SECRETS AND CONFIDENTIAL INFORMATION.**

105. On August 29, 2019, the United States Attorney Office, acting through its employees the Federal defendants Rosa Emilia Rodriguez-Velez, AUSA Jose Capo-Irriarte, AUSA Nicholas W. Canon, instructed Federal defendants Lance Lange, Kevin Pearson to return for a second time with the Dish Network defendants acting through its employees, the defendants Jordan Smith and Kevin Gedeon posing as federal agents to Naicom's Data Center. The Dish Network defendants acting through its employees, defendants Jordan Smith and Kevin Gedeon using the keys that defendant Bert Eichhorn misappropriated from Naicom's Offices without authorization entered its premises located at Villa Fontana, 4SS N2 Via Josefina, Carolina, PR 00983 to resume the misappropriation of the intellectual property, trade secrets and confidential information from Naicom's Data Center computers, and servers.

106. Upon the Dish Network defendants almost completing its second illegal search and unauthorized intrusion and acces, of the Naicom's Data Center computers, servers

and other hardware equipment for prolonged hours, Federal defendant Kevin Pearson decided to contact Naicom employee Jaime Echevarria at his cell phone and ordered him to show up at the Data Center under the ruse that he wanted to interrogate him, Darwin and Victor.

107. Upon arriving at Data Center Darwin Quinones observed the Dish Network defendants acting through its employees, defendants Jordan Smith and Kevin Gedeon still posing as federal agents, accessing Naicom's Data Center computers, servers, other hardware equipment containing Intellectual Property, Trade Secrets and Confidential Information without authorization.

108. During the execution of the warrantless search defendants Kevin Pearson and Lance Lange instead of interrogating Darwin Quinones, began to pressure him into signing a hold harmless document accepting he was running a pirate operation in the past so that they could close the case or else his boss had given him orders to shut down the Data Center operation.

109. Darwin Quinones rejected the proposition outright, and defendants Kevin Pearson and Lance Lange implored Darwin Quinones to sign the document so that they could close the case or else they were going to have problems, but Darwin Quinones again refused to do so.

110. Sometime thereafter, Mr. Vega showed up at the scene and upon entering the Data

Center asked defendants Kevin Pearson and Lance Lange if they had another search warrant to enter and search the Data Center. Defendant Lance Lange represented to Mr. Vega that the search warrant gave him ten (10) days to come in and out to search the Data Center, although, the probable cause, dissipated the moment they executed and concluded the first search, fruitless and with no criminal information to report. Mr. Vega reacted and told defendant Lance Lange to leave Naicom's Data Center premises because he was violating the United States Constitution and Federal law.

111. At that time, Mr. Vega informed defendants Kevin Pearson and Lance Lange that he had already discovered via LinkedIn that the alleged FBI experts who executed the search and seizure warrants at Naicom, Artist Designs, Kiaras, LLC and Naicom's Data Center, who interrogated him, and Darwin Quinones at the FBI Offices were Kevin Gedeon, investigator of Dish Network and Jordan Smith, Bert Eichhorn and Emily Rinkle investigators of NagraStar.

112. Mr. Vega also questioned defendants Lance Lange and Kevin Pearson as to why they brought his competition to search, inspect and photograph confidential information and allowed them to access computers and servers containing trade secrets codes sources, business and intellectual property information belonging to the Plaintiff's corporations.

113. The Dish Network and Federal defendants insisted to continue with the execution

of the warrantless search, unauthorized intrusion and access into Naicom's Data Center computers and servers, and Mr. Vega called his Attorney and notified him that the FBI agents were executing a second warrantless search and seizure at Naicom's Data Center, and after speaking to defendant Lance Lange, the defendants shut down Naicom's business operation and left the premises.

**VIII. THE DEMAND FOR RETURN OF PROPERTY CONTAINING CONFIDENTIAL INFORMATION UNDER RULE 41(G)**

114. On September 6, 2019, a Motion for DEMAND for Return of Seized Property was filed Pursuant to Federal Rules of Criminal Procedure 41(g) ("The Rule 41(g) Motion") by Rafael F. Castro-Lang on behalf of Artist Designs and Management Corporation, Kiaras, LLC, Naicom Corporation, Naicom Data Center, Darwin Quinones-Pimentel, Victor Vega-Encarnacion ("The Plaintiffs"). [D.E. 1 Civil Docket 3:19-mc-00308-FAB].

115. In the Rule 41(g) Motion Plaintiff's contended that the Search and Seizure was unlawful and illegally issued because; (1) it contained deliberate, reckless false statements made under oath and affirmation to secure its issuance by the Magistrate Judge; (2) and therefore was issued in violation of the Fourth Amendment; (3) requiring the immediate return of all the property seized.

116. Furthermore, the Rule 41(g) Motion contained independent evidence in the form of attachments of Naicom's Corporation's contracts authorizing the distribution of content programming in Puerto Rico, United States and the Virgin Islands, and

evidence disproving that the defendant never called HBO or NRTC inquiring about Naicom, and evidence disproving any money laundering activities, and that the criminal investigation was nothing more than a ruse orchestrated by Nagrastar and Dish Network to use the Federal Bureau of Investigations as an instrument to enter Naicom Corporation and the Data Center through a search warrant and misappropriate themselves with Naicom's trade secrets and intellectual property. [D.E. 1 Civil Docket 3:19-mc-00308-FAB].

117. On October 15, 2019, The United States filed an unopposed response to Plaintiff's Rule 41(g) Motion, stating that without conceding any arguments raised, the property items listed in his request would be returned. [D.E. 9-page 1 Civil Docket 3:19-mc-00308-FAB].

118. On November 5, 2019, the District Court granted Plaintiff's Rule 41(g) Motion and entered the following; ("ORDER re 12 Notice (Other), re 10 Report and Recommendation, re 1 Motion for Return of Property: NOTED. Claimant having waived the 14-day period to file objections to the Report and Recommendation (R&R), the Court ADOPTS the R&R and orders the government to return the property listed in claimant's demand. (Docket No. 1)" pursuant to Rule 41 of the Federal Rules of Criminal Procedures. [D.E. 12 and 13 Civil Docket 3:19-mc-00308-FAB].

119. The Government never opposed nor denied that the underlying basis for the search warrant were false and the search warrant against plaintiffs 'was dismissed on the

government's own motion. [D.E. 9-page 1 Civil Docket 3:19- mc-00308-FAB].

**IX. THE SIGNIFICANT HARM INFILCTED UPON PLAINTIFFS.**

120. The defendant's intrusion into Victor Vega, Darwin Quinones, Naicom Corporation, the Data Center, Paylink and Kiaras, LLC privacy and business under the ruse of a criminal investigation caused significant damages to Plaintiffs.
121. Prior to the execution of the search warrants, the Plaintiffs' enjoyed a great reputation and were about to close an investment deal of \$15,000,000 dollars to advance Naicom's goals to the next level of launching the brand in the United States by 2019 in the States of Florida and New York.
122. When the investors found out that Naicom Corporation and its executive officers were under criminal investigation and that their offices were raided by the FBI, the investors emailed Darwin Quinones that they were abandoning the negotiations due to the pending criminal investigation.
123. Naicom Corporation was also about to close a multimillion contract with Claro Puerto Rico by August 2018. When the executive officers of Claro Puerto Rico found out through Dish Network that the FBI was investigating Naicom Corporation and that their executive officers were about to be arrested and prosecuted, and Naicom was about to be dismantled for running an illegal IPTV pirate content distribution operation, Claro Puerto Rico pulled out of the negotiations and never again contacted Naicom's executive officers to renew them.

124. In the aftermath of the search warrant execution of Naicom's Data Center, Naicom lost a great deal of subscribers because of the negative reputation caused by the defendants. Furthermore, the Dish Netwrok and Federal defendants intrusion into Naicom's Data Center computers, servers and other equipment caused enormous damages to the Data Center computer's and server's system leaving many subscribers without tv programming services for weeks, causing Plaintiffs the expense of having spent thousands of dollars and man hours resources in repairing and acquiring new equipment due to the damages caused by the defendants.

### **CAUSES OF ACTION**

#### **COUNT ONE RICO (18 U.S.C. § 1962(C)) (AGAINST ALL DEFENDANTS)**

125. Plaintiff realleges and incorporates by reference all prior paragraphs of this Complaint and paragraphs in the counts below as set forth fully herein.

126. Defendants are all "persons" within the meaning of 18 U.S.C. § 1961(3). At all relevant times, Defendants associated themselves in fact and conducted the affairs of an Enterprise—which affected interstate commerce—through a pattern of racketeering activity, in violation of 18 U.S.C. § 1962(c).

##### **A. The Dish Network Corporation Was The Racketeering Enterprise.**

127. The Dish Network Corporation was a Racketeering Enterprise, as that term is used in 18 U.S.C. § 1961(4).

128. The Dish Network defendants had an ongoing organization framework for carrying out its objectives.
129. As described above, each defendant participated in the operation or management of the Enterprise.
130. The Dish Network Corporation was an Association-In-Fact Enterprise comprising Dish Network, LLC, NagraStar, LLC, Bert Eichhorn, Jordan Smith, Kevin Gedeon, the United States Attorney's Office For The District Of Puerto Rico, through its employees U.S. Attorney Rosa Emilia Rodriguez-Velez, AUSA Jose Capo-Irriarte, AUSA Nicholas W. Cannon, and the Federal Bureau Of Investigation, San Juan, Field, Puerto Rico; through its employees, FBI SPECIAL AGENTS Douglas A. Leff, Bradley Rex, Lance Lange, Kevin Reaves, Clay Rehrig, Juan Galarza, Several Unknown Named Agents of the Federal Bureau Of Investigations, and John Does 1-20.
131. The Dish Network defendants', employees, agents and additional legal entities such as the United States Attorney Office For The District Of Puerto Rico, acting though its employees Rosa Emilia Rodriguez-Velez, AUSA Jose Capo-Irriarte, AUSA, Nicholas W. Cannon and the Federal Bureau Of Investigation, San Juan, Field, Puerto Rico; acting through its employees, FBI Special Agents Douglas A. Leff, Bradley Rex, Lance Lange, Kevin Reaves, Clay Rehrig, Juan Galarza, Several Unknown Names Agents Of Federal Bureau Of Investigations; John Does 1-20, and

individuals known and unknown formed The Association-In-Fact Enterprise by July 2017 or, at the very least, by June 2017. From the date the Enterprise was formed until the present, the members of the Association-In-Fact Enterprise have worked together to further their mutual goal of depriving Plaintiffs of their Confidential Information to secure Dish Network the theft of Plaintiffs' D&V IP Holdings' and Naicom's Corporation of DISME's technology and Intellectual Property and Trade Secrets.

132. The Association-In-Fact Enterprise had an ongoing organizational framework for carrying out its objectives. The Association-In-Fact Enterprise could not have carried out its intricate task of attempting or stealing Plaintiffs' Intellectual Property and Trade Secrets when it did unless it had some structure for making and communicating group decisions, and using the powers of the United States Attorney Office For The District Of Puerto Rico, through its employees U.S. Attorney Rosa Emilia Rodriguez-Velez, AUSA Jose Capo-Irriarte, AUSA Nicholas W. Cannon, and the powers of the Federal Bureau Of Investigation, San Juan, Field, Puerto Rico, through its employees, FBI Special Agents Douglas A. Leff, Bradley Rex, Lance Lange, Kevin Reaves, Clay Rehrig, Juan Galarza, Several Unknown Names Agents Of Federal Bureau Of Investigations; John Does 1-20, to accomplish its goals.

133. As described above, Dish Network and Federal defendants participated in the

operation or management of the Association-In-Fact Enterprise, either by attempting to steal or stealing the DISME technology, and benefitting from its technology in the form of misappropriating Plaintiffs' from their Intellectual Property/Trade Secrets, gain economic value, while the Federal defendants facilitated the Dish Network defendants the means of committing the attempted or theft of Plaintiffs' Intellectual Property/Trade Secrets, for political gain, and destroying Plaintiffs' corporation.

134. Because the Association-In-Fact Enterprise's activities affected Naicom's IPTV television programming transmission, distribution and services through the internet and private networks, it affected interstate and foreign commerce.

### C. RICO Predicate Acts

135. Each Defendant conducted and/or participated in the affairs of the Dish Network defendants goals and objectives and the Association-In-Fact Enterprise through a pattern of racketeering activity, including acts indictable under Mail Fraud (18 U.S.C. § 1341), Wire Fraud (18 U.S.C. § 1343), Conspiracy To Commit Mail And Wire Fraud (18 U.S.C. § 1341), Theft Of Trade Secrets Under The Defend Trade Secrets Act (18 U.S.C. § 1836 et seq.), while in addition, committing the possible underlying criminal offenses as prohibited under Fraud and Abuse Act (18 U.S.C. § 1030(a)); Stored Communications Act (18 U.S.C. §§ 2701-12); Digital Millennium Copyright Act (17 U.S.C. § 1201 et seq.), 18 U.S.C.A. § 2235- Search warrant procured

maliciously; 18 U.S.C.A. § 1621- Perjury generally; 18 U.S.C.A. § 1001- Statements or entries generally, 18 U.S.C.A. § 912- Officer or employee of the United States; 18 U.S.C.A. § 2234- Authority exceeded in executing warrant; 18 U.S.C.A. § 2236- Searches without warrant, 18 U.S.C.A. § 1905- Disclosure of Confidential Information, while accomplishing their racketeering objectives.

**a. The Mail Fraud**

136. On August 7, 2017, the Dish Network defendants acting through its employees, defendants Kevin Gedeon, Jordan Smith, Bert Eichhorn, Emily Rinkle, Brian Parsons, and under the supervision, and powers of the United States Attorney's Office for The District Of Puerto Rico, though its employees, U.S.A. Rosa Emilia Rodriguez-Velez, AUSA Jose Capo-Irriarte, AUSA Nicholas W. Cannon, and supervision, direction and powers of the Federal Bureau Of Investigation, San Juan, Field, Puerto Rico; acting through its employees, FBI Special Agents Douglas A. Leff, Bradley Rex, Lance Lange, Kevin Reaves, Clay Rehrig, Juan Galarza, Several Unknown Names Agents Of Federal Bureau Of Investigations, John Does 1-20 instructed Brian Parsons to purchase a Naicom TV Set Top Box receiver to defraud Naicom under the pretense that Brian Parsons was in fact a Naicom IPTV customer, when the Dish Network defendant's intention was solely to conduct espionage by reverse engineering on Naicom's IPTV Set Top Box middle firmware in their attempt to misappropriate themselves with Naicom's intellectual property and trade secrets. The Dish Network and Federal defendants accomplished the scheme

through Brian Parsons, who placed the order via Naicom's website, registered online, and had the Naicom IPTV Set Top Box mailed to him at the following Address: 9079 FOURTHSTREET NORTH SAINTPETERS FL 33702 via the United States Postal Service.

**b. The Wire Fraud**

137. On August 7, 2017, the Dish Network defendants acting through its employees, defendants Kevin Gedeon, Jordan Smith, Bert Eichhorn, Emily Rinkle, Brian Parsons, and under the supervision and powers of the United States Attorney Office For The District Of Puerto Rico, acting though its employees U.S.A. Rosa Emilia Rodriguez-Velez, AUSA Jose Capo-Irriarte, AUSA Nicholas W. Cannon, and the supervision and powers of the Federal Bureau Of Investigation, San Juan, Field, Puerto Rico; acting through its employees, FBI Special Agents Douglas A. Leff, Bradley Rex, Lance Lange, Kevin Reaves, Clay Rehrig, Juan Galarza, Several Unknown Names Agents Of Federal Bureau Of Investigations, John Does 1-20 instructed Brian Parsons to purchase a Naicom IPTV Set Top Box receiver to defraud Naicom under the pretense that Brian Parsons was in fact a Naicom IPTV potential customer, when the Dish Network and Federal defendants' intentions was solely to commit reverse engineering tests on Naicom's IPTV Set Top Box middle firmware in their attempt to misappropriate themselves with D&V IP Holdings DISME technology and Naicom's corporations intellectual property and trade secrets. The Dish Network and Federal defendants accomplished the scheme

though Brian Parsons, who not only placed the order via Naicom's website, but also used the internet to register online the following information: BRIAN PARSONS, Phone (727)409-9464, Email: [parsons.brian716@outlook.com](mailto:parsons.brian716@outlook.com) Address: 9079 FOURTHSTREET NORTH SAINTPETERS FL 33702 IP: 70.127.233.139, and made online payments through the internet using the PM Visa ending in 2775, and purchased two Naicom's IPTV set top boxes, MAC Numbers 00:1A:79:46:97:AD; and 00:1A:79:46:A4:BE which were mailed to Brian Parsons residence, via the United States Postal Service, to the above address.

138. The Dish Network and Federal defendants maintained their fraudulent scheme of spying and conducting reverse engineering on Naicom's IPTV Set Top Box middle firmware from 2017 up to 2019 (two years), through the Dish Network defendants employees, and defendant Brian Parsons, who was in charge of making the payments online through the internet using his PM Visa ending in 2775, making 22 fraudulent payments and wiring to Naicom IPTV the total amount of \$1,304.81 for the alleged Naicom's IPTV services.

139. The Dish Network and Federal defendants maintained the continuing fraudulent scheme from 2017 up to 2019 (two years), through defendant Brian Parsons, who made payments online through the internet using his PM Visa ending in 2775, making 22 fraudulent payments and wiring a Naicom IPTV the total amount of \$1,304.81 to for Naicom's IPTV alleges services, knowingly and intentionally to commit mail fraud as that offense is prohibited under 18 U.S.C. § 1343.

140. See table below reflecting Brian Parsons wired transactions

Transaction of Brain Parsons Customer 1745

<b>Order Number</b>	<b>ClientID</b>	<b>order date</b>	<b>delivery</b>	<b>amount</b>
<b>195</b>	1745	2017-08-07 15:32:49	Shipping	\$130.00
<b>271</b>	1745	2018-01-25 19:27:11	Shipping	\$130.00
<b>345</b>	1745	2018-03-07 16:53:23	Digital	\$54.99
<b>492</b>	1745	2018-05-14 13:18:15	Digital	\$54.99
<b>585</b>	1745	2018-06-10 17:16:39	Digital	\$54.99
<b>664</b>	1745	2018-07-10 08:38:15	Digital	\$54.99
<b>763</b>	1745	2018-08-11 09:00:02	Digital	\$54.99
<b>805</b>	1745	2018-08-24 20:22:45	Digital	\$54.99
<b>899</b>	1745	2018-09-23 09:00:21	Digital	\$54.99
<b>931</b>	1745	2018-09-28 14:58:49	Digital	0
<b>932</b>	1745	2018-09-28 15:02:34	Digital	\$54.99
<b>1022</b>	1745	2018-10-27 15:49:32	Digital	\$54.99
<b>1119</b>	1745	2018-11-25 14:43:35	Digital	\$54.99
<b>1213</b>	1745	2018-12-23 14:06:42	Digital	\$54.99
<b>1308</b>	1745	2019-01-21 16:32:11	Digital	\$54.99
<b>1424</b>	1745	2019-02-19 07:35:11	Digital	\$54.99
<b>1550</b>	1745	2019-03-24 09:00:02	Digital	\$54.99
<b>1671</b>	1745	2019-04-21 15:00:45	Digital	\$54.99
<b>1800</b>	1745	2019-05-21 00:12:04	Digital	\$54.99
<b>1934</b>	1745	2019-06-22 09:00:02	Digital	\$54.99
<b>2043</b>	1745	2019-07-22 09:00:01	Digital	\$54.99
<b>2185</b>	1745	2019-08-21 09:00:02	Digital	\$54.99

### c. The Mail and Wire Fraud Conspiracy

141. The factual allegations in paragraphs 134 and 135 including the scheme to defraud

set out therein, are realleged and incorporated herein as if set forth in full. The Dish Network defendants acting through its employees, defendants Kevin Gedeon, Jordan Smith, Bert Eichhorn, Emily Rinkle, Brian Parsons, and under the supervision and powers of the United States Attorney Office For The District Of Puerto Rico, acting though its employees U.S.A. Rosa Emilia Rodriguez-Velez, A USA Jose Capo-Irriarte, AUSA Nicholas W. Cannon, and supervision and powers of the Federal Bureau Of Investigation, San Juan, Field, Puerto Rico; acting through its employees , FBI Special Agents Douglas A. Leff, Bradley Rex, Lance Lange, Kevin Reaves, Clay Rehrig, Juan Galarza, Several Unknown Names Agents Of Federal Bureau Of Investigations; John Does 1-20, did knowingly and intentionally conspire and agree with each other to commit mail and wire fraud offenses described herein all in violation of 18 U.S.C. § 1341 and 1343 and 1349.

**d. Theft of Trade Secrets**

142. Beginning on or before August 7, 2017, the Dish Network defendants acting through its employees, defendants Kevin Gedeon, Jordan Smith, Bert Eichhorn, Emily Rinkle, Brian Parsons, and under the supervision of the powers of the United States Attorney Office For The District Of Puerto Rico, acting though its employees, U.S.A. Rosa Emilia Rodriguez-Velez, AUSA Jose Capo-Irriarte, AUSA Nicholas W. Cannon, and the supervision and powerS of the Federal Bureau Of Investigation, San Juan, Field, Puerto Rico, acting through its employees, FBI Special Agents

Douglas A. Leff, Bradley Rex, Lance Lange, Kevin Reaves, Clay Rehrig, Juan Galarza, Several Unknown Names Agents Of Federal Bureau Of Investigations; John Does 1-20 repeatedly attempted—in many instances successfully—to steal, and without authorization appropriate, take, carry away, or by fraud, artifice, or deception obtain trade secrets from D&V IP Holdings and Naicom's corporation, with the intent to convert those trade secrets, which are and were related to products or services used in or intended for use in interstate commerce, to the economic benefit of Dish Network defendants and non-defendant coconspirators, and intending and knowing that the offense would injure D&V IP Holdings and Naicom's corporation, in violation of 18 U.S.C. § 1832(a)(1) and (a)(4).

143. Beginning on or before August 7, 2017, the Dish Network defendants, acting through its employees, defendants Kevin Gedeon, Jordan Smith, Bert Eichhorn, Emily Rinkle, Brian Parsons, and under the supervision and powers of the United States Attorney Office For The District Of Puerto Rico, acting though its employees U.S.A. Rosa Emilia Rodriguez-Velez, AUSA Jose Capo-Irriarte, AUSA Nicholas W. Cannon, and the supervision and powers of the Federal Bureau Of Investigation, San Juan, Field, Puerto Rico, acting through its employees, FBI Special Agents Douglas A. Leff, Bradley Rex, Lance Lange, Kevin Reaves, Clay Rehrig, Juan Galarza, Several Unknown Names Agents Of Federal Bureau Of Investigations, and John Does 1-20 did without authorization, spy, reverse engineered, copied,

duplicated, downloaded, uploaded, altered, destroyed, replicated, transmitted, delivered, sent, communicated, and/or conveyed trade secrets from D&V IP Holdings and Naicom's corporation, with the intent to convert those trade secrets, which are related to products or services used in or intended for use in interstate commerce, to the economic benefit of the Dish Network defendants and non-defendant coconspirators, intending and knowing that the offense would injure D&V IP Holdings and Naicom's corporation, in violation of 18 U.S.C. § 1832(a)(2).

144. Beginning on or before August 7, 2017, the Dish Network defendants acting through its employees, defendants Kevin Gedeon, Jordan Smith, Bert Eichhorn, Emily Rinkle, Brian Parsons, under the supervision and powers of the United States Attorney's Office For The District Of Puerto Rico, acting though its employees U.S.A. Rosa Emilia Rodriguez-Velez, AUSA Jose Capo-Irriarte, AUSA Nicholas W. Cannon, and the powers of the Federal Bureau Of Investigation, San Juan, Field, Puerto Rico, acting through its employees, FBI Special Agents Douglas A. Leff, Bradley Rex, Lance Lange, Kevin Reaves, Clay Rehrig, Juan Galarza, Several Unknown Names Agents Of Federal Bureau Of Investigations, and John Does 1-20, received, bought, or possessed D&V IP Holdings and Naicom's corporation trade secrets, with the intent to convert those trade secrets, which are related to products or services used in or intended for use in interstate commerce, knowing the same to have been stolen or appropriated, obtained, or converted without authorization, to

the economic benefit of itself and the other Defendants and non-defendant coconspirators, intending and knowing that the offense would injure the D&V IP Holdings, Naicom, Kiaras And Paylink Corporations , in violation of 18 U.S.C. § 1832(a)(3).

145. On August 27 and 29, of 2019, the United States Attorney Office For The District Of Puerto Rico, acting though its employees U.S.A. Rosa Emilia Rodriguez-Velez, AUSA Jose Capo-Irriarte, AUSA Nicholas W. Cannon, the Federal Bureau Of Investigation, San Juan, Field, Puerto Rico, acting through its employees, FBI Special Agents Douglas A. Leff, Bradley Rex, Lance Lange, Kevin Reaves, Clay Rehrig, Juan Galarza, Several Unknown Names Agents Of Federal Bureau Of Investigations, and John Does 1-20 the Federal defendants, facilitated and allowed the Dish Network defendants, without authorization, the access to trade secrets from D&V IP Holdings DISME technology and Naicom's corporation, with the intent to facilitate the Dish Network defendants the opportunity to convert those trade secrets, which are and were related to products or services used in or intended for use in interstate commerce, to the economic benefit of Dish Network and the other Dish Network defendants, and intending and knowing that the offense would injure D&V IP Holdings and Naicom's corporation, under the supervision and power oof the United States Attorney Office and the Federal Bureau of Investigations, San Juan, Field For The District Of Puerto Rico, in violation of 18

U.S.C. § 1832(a)(2).

**RICO DAMAGES.**

146. Plaintiffs have been injured in its business and property by Defendants' violation of 18 U.S.C. § 1962(c). Defendants caused enormous harm to Plaintiff's business, as described above, and to Plaintiff's computers and servers. All of these injuries occurred within the United States.

**COUNT TWO**  
**RICO CONSPIRACY (18 U.S.C. § 1962(D))**  
**(AGAINST ALL DEFENDANTS)**

147. Plaintiff realleges and incorporates by reference all prior paragraphs of this Complaint and those in the counts below as though set forth fully herein.

148. Defendants conspired with each other to violate 18 U.S.C. § 1962(c). Defendants knowingly agreed, combined, and conspired to conduct the affairs of the Enterprise or the Association-In-Fact Enterprise to attempt or commit theft of trade secrets through a hoax criminal investigation operation. Each Defendant agreed that the operation would involve repeated violations of Mail Fraud (18 U.S.C. § 1341), Wire Fraud (18 U.S.C. § 1343), Conspiracy To Commit Mail And Wire Fraud (18 U.S.C. § 1341), Theft Of Trade Secrets Under The Defend Trade Secrets Act (18 U.S.C. § 1836 et seq.), involving the commission of underlying criminal offenses of the Fraud and Abuse Act (18 U.S.C. § 1030(a)); Stored Communications Act (18 U.S.C. §§ 2701-12); Digital Millennium Copyright Act (17 U.S.C. § 1201 et seq.), 18 U.S.C.A. § 2235-

Search warrant procured maliciously: 18 U.S.C.A. § 1621- Perjury generally, 18 U.S.C.A. § 1001- Statements or entries generally, 18 U.S.C.A. § 912- Officer or employee of the United States; 18 U.S.C.A. § 2234- Authority exceeded in executing warrant; 18 U.S.C.A. § 2236- Searches without warrant, 18 U.S.C.A. § 1905- Disclosure of Confidential Information, while accomplishing their conspiratorial racketeering objectives, all in violation of 18 U.S.C. § 1962(c) and § 1962(d).

149. Plaintiffs have been injured in their business or property by Defendants' violation of 18 U.S.C. § 1962(d). Plaintiff has been injured in its business and property by Defendants' violation of 18 U.S.C. § 1962(c). Defendants caused enormous harm to Plaintiff's business, as described above, and to Plaintiff's computers and servers. All of these injuries occurred within the United States.

**COUNT THREE**  
**COMPUTER FRAUD AND ABUSE ACT**  
**(18 U.S.C. § 1030(A))**  
**(AGAINST ALL DEFENDANTS)**

150. Plaintiff realleges and incorporates by reference all prior paragraphs of this Complaint and paragraphs in the counts below as though set forth fully herein.

151. The Naicom Offices and Data Center computers are involved in interstate and foreign commerce and communication, and are protected computers under 18 U.S.C. § 1030(e)(2).

152. On August 27 and 29, 2019, The Dish Network defendants acting through its employees, defendants Kevin Gedeon, Jordan Smith, Bert Eichhorn, Emily Rinkle, Brian Parsons, and under the supervision and powers of the United States Attorney Office For The District Of Puerto Rico, acting though its employees. U.S.A. Rosa Emilia Rodriguez-Velez, AUSA Jose Capo-Irriarte, AUSA Nicholas W. Cannon, and supervision and powers of the Federal Bureau Of Investigation, San Juan, Field, Puerto Rico, acting through its employees, FBI Special Agents Douglas A. Leff, Bradley Rex, Lance Lange, Kevin Reaves, Clay Rehrig, Juan Galarza, Several Unknown Names Agents Of Federal Bureau Of Investigations; John Does 1-20,did knowingly and intentionally access the Naicom Offices and Data Center computers without authorization or in excess of authorization, obtained and used valuable information from those computers in violation of 18 U.S.C. § 1030(a)(2)(C). Such information included, but was not limited to intellectual property, trade secrets and confidential information. The information was used to advance defendants Dish Network's economic advantage and destroy Plaintiffs' business.

153. Upon information and belief, The Dish Network defendants acting through its employees, defendants Kevin Gedeon, Jordan Smith, Bert Eichhorn, Emily Rinkle, Brian Parsons, and under the supervision and powers of the United States Attorney Office For The District Of Puerto Rico, acting though its employees, U.S.A. Rosa Emilia Rodriguez-Velez, AUSA Jose Capo-Irriarte, AUSA Nicholas W. Cannon, and supervision and powers of the Federal Bureau Of Investigation, San Juan, Field,

Puerto Rico, acting through its employees, FBI Special Agents Douglas A. Leff, Bradley Rex, Lance Lange, Kevin Reaves, Clay Rehrig, Juan Galarza, Several Unknown Names Agents Of Federal Bureau Of Investigations, and John Does 1-20, did knowingly cause the transmission of information or a program, code, or command, and as a result of such conduct, intentionally caused damage without authorization to a protected computer, in violation of 18 U.S.C. § 1030(a)(5)(A). Such transmission included, but was not limited to, the use of malware on Naicom Offices and Data Center computers systems.

154. Upon information and belief, the Dish Network defendants acting through its employees, defendants Kevin Gedeon, Jordan Smith, Bert Eichhorn, Emily Rinkle, Brian Parsons, and under the supervision and powers of the United States Attorney's Office For The District Of Puerto Rico, acting though its employees U.S.A. Rosa Emilia Rodriguez-Velez, AUSA Jose Capo-Irriarte, AUSA Nicholas W. Cannon, and supervision and powers of the Federal Bureau Of Investigation, San Juan, Field, Puerto Rico; acting through its employees, FBI Special Agents Douglas A. Leff, Bradley Rex, Lance Lange, Kevin Reaves, Clay Rehrig, Juan Galarza, Several Unknown Names Agents Of Federal Bureau Of Investigations, and John Does 1-20, did intentionally access a protected computer or computers without authorization, and as a result of such conduct, caused damage and loss, in violation of 18 U.S.C. § 1030(a)(5)(C) and 18 U.S.C. § 1030(a)(5)(B) to D&V IP Holdings and Naicom corporations.

155. The Dish Network defendants acting through its employees, defendants Kevin Gedeon, Jordan Smith, Bert Eichhorn, Emily Rinkle, Brian Parsons, and under the supervision and powers of the United States Attorney Office For The District Of Puerto Rico, acting though its employees U.S.A. Rosa Emilia Rodriguez-Velez, AUSA Jose Capo-Irriarte, AUSA Nicholas W. Cannon, and supervision and powers of the Federal Bureau Of Investigation, San Juan, Field, Puerto Rico, acting through its employees, FBI Special Agents Douglas A. Leff, Bradley Rex, Lance Lange, Kevin Reaves, Clay Rehrig, Juan Galarza, Several Unknown Names Agents Of Federal Bureau Of Investigations, and John Does 1-20, caused loss to one or more persons during a one-year period aggregating well over \$5,000 in value, and they also caused damage affecting ten or more protected computers during a one-year period.
156. The Naicom Corporation suffered damageS and loss as a consequence of the Dish Network and Federal defendants' actions, including but not limited to the cost of investigating and responding to the unauthorized access and abuse of their computer networks, conducting damage assessments, restoring and replacing computers and data, programs, systems, or information, the loss of the value of the D&V IP Holdings and Naicom's trade secrets, and the harm to Naicom's business as described above. The D&V IP HOLDINGS, NAICOM, KAIRAS AND PAYLINK CORPORATIONS seeks compensatory and other equitable relief under 18 U.S.C. § 1030(g).

**COUNT FOUR**

**STORED COMMUNICATIONS ACT  
(18 U.S.C. §§ 2701-12)  
(AGAINST ALL DEFENDANTS)**

157. Plaintiffs reallege and incorporate by reference all prior paragraphs of this Complaint and paragraphs in the counts below as though set forth fully herein.
158. Plaintiffs is a “person” within the meaning of 18 U.S.C. §§ 2510(6) and 2707(a).
159. The Dish Network defendants acting through its employees, defendants Kevin Gedeon, Jordan Smith, Bert Eichhorn, Emily Rinkle, Brian Parsons, and under the supervision and powers of the United States Attorney’s Office For The District Of Puerto Rico, acting though its employees U.S.A. Rosa Emilia Rodriguez-Velez, AUSA Jose Capo-Irriarte, AUSA Nicholas W. Cannon, and supervision and powers of the Federal Bureau Of Investigation, San Juan, Field, Puerto Rico, acting through its employees, FBI Special Agents Douglas A. Leff, Bradley Rex, Lance Lange, Kevin Reaves, Clay Rehrig, Juan Galarza, Several Unknown Names Agents Of Federal Bureau Of Investigations, and John Does 1-20, willfully and intentionally accessed without authorization a facility through which an electronic communication service is provided, namely, the D&V IP Holdings, Naicom’s IPTV, Kiaras’ and Paylink’s services and computer systems, including their email servers, thereby obtaining access to wire or electronic communications while they were in electronic storage in such systems, in violation of 18 U.S.C. § 2701(a).
160. As a result of these willful and intentional violations, Plaintiff has suffered damages and, as provided for in 18 U.S.C. § 2707, seeks an award of the greater of the actual

damages suffered or the statutory damages; punitive damages; attorneys' fees and other costs of this action; and appropriate equitable relief.

**COUNT FIVE**

**DIGITAL MILLENNIUM COPYRIGHT ACT  
(17 U.S.C. § 1201 ET SEQ.)**

161. Plaintiff realleges and incorporates by reference all prior paragraphs of this Complaint and paragraphs in the counts below as though set forth fully herein.
162. Plaintiff's computer networks and files contained information subject to protection under the copyright laws of the United States, including software programs, documents, confidential information and research.
163. On August 27 and 29, 2019, the Dish Network defendants acting through its employees the defendants Kevin Gedeon, Jordan Smith, Bert Eichhorn, Emily Rinkle, Brian Parsons, and under the supervision and powers of the United States Attorney Office For The District Of Puerto Rico, acting though its employees, U.S.A. Rosa Emilia Rodriguez-Velez, AUSA Jose Capo-Irriarte, AUSA Nicholas W. Cannon, and supervision and powers of the Federal Bureau Of Investigation, San Juan, Field, Puerto Rico, acting through its employees, FBI Special Agents Douglas A. Leff, Bradley Rex, Lance Lange, Kevin Reaves, Clay Rehrig, Juan Galarza, Several Unknown Names Agents Of Federal Bureau Of Investigations, and John Does 1-20, illegally accessed without authorization, the Paylink Corporation copyrighted material contained in Paylink's computer software programs, systems, and

networks controlled by technological measures, including measures restricting remote access, firewalls, and measures restricting access to users with valid credentials and passwords.

164. The Dish Network defendants acting through its employees, defendants Kevin Gedeon, Jordan Smith, Bert Eichhorn, Emily Rinkle, Brian Parsons, and under the supervision and powers of the United States Attorney's Office For The District Of Puerto Rico, acting though its employees U.S.A. Rosa Emilia Rodriguez-Velez, AUSA Jose Capo-Irriarte, AUSA Nicholas W. Cannon, and supervision and powers of the Federal Bureau Of Investigation, San Juan, Field, Puerto Rico, acting through its employees, FBI Special Agents Douglas A. Leff, Bradley Rex, Lance Lange, Kevin Reaves, Clay Rehrig, Juan Galarza, Several Unknown Names Agents Of Federal Bureau Of Investigations, and John Does 1-20, circumvented these technological measures by introducing pen drives into D&V IP Holdings and Naicom's computers and servers, and conducting "password dump" by unlawfully performing passwords resets into the Ubuntu controlling system, changing credentials from authorized users, conducting an access to the D&V IP Holdings and Naicom's domains, in violation of 17 U.S.C. § 1201(a).

165. The Dish Network defendants and Federal defendant's conduct caused Plaintiff significant damages. These damages include, but are not limited to, damage resulting from harm to Paylink's computers and servers, loss in the value of D&V IP Holdings and Naicom's trade secrets and confidential business information, and

harm to the business as described above. Plaintiff is entitled to the greater of its actual damages or statutory damages as provided by 17 U.S.C. § 1203, in an amount to be proven at trial.

166. Plaintiff is entitled to an award of attorneys' fees and costs as provided by 17 U.S.C. § 1203.

**COUNT SIX**

**MISAPPROPRIATION OF TRADE SECRETS  
UNDER THE DEFEND TRADE SECRETS ACT  
(18 U.S.C. § 1836 ET SEQ.)**

167. Plaintiff realleges and incorporates by reference all prior paragraphs of this Complaint and paragraphs in the counts below as though set forth fully herein.

168. The DISME technology, Intellectual Property and Confidential Information that the Dish Network defendants attempted to misappropriate, or actually misappropriated from D&V IP Holdings, and Naicom's Corporation, acting through its employees, defendants Kevin Gedeon, Jordan Smith, Bert Eichhorn, Emily Rinkle, Brian Parsons, and under the supervision and powers of the United States Attorney's Office For The District Of Puerto Rico, acting though its employees U.S.A. Rosa Emilia Rodriguez-Velez, AUSA Jose Capo-Irriarte, AUSA, Nicholas W. Cannon, and supervision and powers of the Federal Bureau Of Investigation, San Juan, Field, Puerto Rico, acting through its employees, FBI Special Agents Douglas A. Leff, Bradley Rex, Lance Lange, Kevin Reaves, Clay Rehrig, Juan Galarza, Several

Unknown Names Agents Of Federal Bureau Of Investigations, and John Does 1-20, include trade secrets within the meaning of 18 U.S.C. § 1839.

169. Specifically, the D&V IP Holdings and Naicom Corporation are in the business of networks and internet communications, IPTV business, and the misappropriation of the confidential and digital information, D&V IP Holdings' DISME technology, Naicom's, Kiaras' and Paylink's trade secrets, research, and business strategic and other confidential information essential to the future of Plaintiffs' Corporations.

170. As described above D&V IP Holdings and Naicom takes and has taken reasonable measures to keep such confidential information protected and secret.

171. Plaintiff's trade secrets were related to products or services used in, or intended for use in, interstate or foreign commerce.

172. The Dish Network defendants acting through its employees, defendants Kevin Gedeon, Jordan Smith, Bert Eichhorn, Emily Rinkle, Brian Parsons, misappropriated Plaintiff's trade secrets, knowing or having reason to know that the trade secrets were being acquired by improper means, and under the supervision and powers of the United States Attorney Office For The District Of Puerto Rico, acting though its employees U.S.A. Rosa Emilia Rodriguez-Velez, AUSA Jose Capo-Irriarte, AUSA Nicholas W. Cannon, and supervision and powers of the Federal Bureau Of Investigation, San Juan, Field, Puerto Rico, acting through its employees, FBI Special Agents Douglas A. Leff, Bradley Rex, Lance Lange, Kevin Reaves, Clay Rehrig, Juan

Galarza, Several Unknown Names Agents Of Federal Bureau Of Investigations, and John Does 1-20, under the hoax of a criminal investigation.

173. As a direct consequence of Defendants' misappropriation, Plaintiff has suffered damages for the cost of materials, loss of goodwill, and attorneys' fees and costs. Plaintiff is also entitled to punitive damages. These damages include, but are not limited to, damage resulting from harm to D&V IP Holdings and Naicom computers and servers, loss in the value of D&V IP Holdings, DISME technology, and Naicom, Kiaras and Paylink trade secrets and business information, and harm to its business as described above.
174. Plaintiff is also entitled to a preliminary and permanent injunction pursuant to 18 U.S.C. § 1836(b)(3).

**COUNT SEVEN**

**PUERTO RICO INDUSTRIAL AND TRADE SECRETE PROTECTION ACT  
UNDER THE UNIFORM TRADE SECRETS ACT  
(LAW NO. 80, OF JUNE 3, 2011)  
(AGAINST ALL DEFENDANTS)**

175. Plaintiff realleges and incorporates by reference all prior paragraphs of this Complaint and paragraphs in the counts below as though set forth fully herein.
176. The Puerto Rico Industrial And Trade Secret Protection Act Under The Uniform Trade Secrets Act empowers a party to recover damages for misappropriation of a trade secret.

177. The Confidential Information the Dish Network defendants acting through its employees, defendants Kevin Gedeon, Jordan Smith, Bert Eichhorn, Emily Rinkle, Brian Parsons, attempted to or misappropriated from Plaintiffs, through the assistance and facilitation of the supervision and powers of the United States Attorney's Office For The District Of Puerto Rico, acting though its employees U.S.A. Rosa Emilia Rodriguez-Velez, AUSA Jose Capo-Irriarte, AUSA Nicholas W. Cannon, and supervision and powers of the Federal Bureau Of Investigation, San Juan Field, Puerto Rico, acting through its employees, FBI Special Agents Douglas A. Leff, Bradley Rex, Lance Lange, Kevin Reaves, Clay Rehrig, Juan Galarza, Several Unknown Names Agents Of Federal Bureau Of Investigations, and John Does 1-20, exfiltrated from the D&V IP Holdings and Naicom computer systems trade secrets under Puerto Rico law, as discussed above, and in keeping with the definition of trade secrets under Puerto Rico law: information, including a formula, pattern, compilation, program, device, method, technique, or process, that: (A) Derives actual or potential independent economic value, from not being generally known, and not being readily ascertainable by proper means by another who can obtain economic value from its disclosure or use; and (B) Is the subject of reasonable efforts to maintain its secrecy, pursuant to Section 11 of Puerto Rico Industrial and Trade Secrets Protection Act (Law No. 80, of June 3, 2011).

178. This information derived an actual independent economic value by remaining confidential and private, and not being readily ascertainable to others. Plaintiff

takes and has taken reasonable measures to keep such information secret, as described and discussed above.

179. Each Defendant disclosed, received, and used these misappropriated trade secrets without Plaintiff's consent, knowing or having reason to know that the trade secrets were acquired by improper means.

180. As a direct consequence of Defendants' attempt or misappropriation, Plaintiff has suffered damages for actual loss and from Defendants' unjust enrichment. These damages include, but are not limited to, damage resulting from harm to D&V IP Holdings, Naicom computers and servers, loss in the value of D&V IP Holdings, Naicom trade secrets and business information, and harm to its business as described above.

181. Defendants' misappropriation of Plaintiff's trade secrets was willful and malicious. Accordingly, Plaintiff is entitled to exemplary damages in an amount up to twice actual damages awarded, as well as attorneys' fees and costs.

#### PRAAYER FOR RELIEF

WHEREFORE, Plaintiff demands judgment against Defendants on all Counts, and seeks such relief as specified below for all Counts for which such relief is provided by law:

- a) Awarding Plaintiff damages in an amount to be determined, including but not limited to all damages and losses suffered by Plaintiff as a result of the illegal attempt to steal or theft, and subsequent release of Plaintiff's confidential information and/or Plaintiff's response to and remediation related thereto;

- b) Awarding Plaintiff compensatory in excess of \$100,000,000 (One Hundred Million dollars) and treble damages, as available, in an amount to be proven at trial;
- c) Awarding Plaintiff the financial gain earned by Defendants as a consequence of the violations described herein;
- d) Awarding Plaintiff statutory damages, as available;
- e) Awarding Plaintiff punitive damages exceeding \$500,000,000 (Five Hundred Million dollars);
- f) Issuing a declaration that; Defendants, according to proof, conspired and engaged in a common scheme to effect the illegal and unauthorized attempt or misappropriation of Plaintiff's computer systems and the exfiltration of confidential information;
- g) Issuing an injunction restraining Defendants and their officers, agents, servants, employees, assigns, and those acting in active concert or participation with them from;
- h) Accessing Plaintiff's computer networks and/or personal emails without Plaintiff's authorization;
- i) Engaging in any activity that disrupts, diminishes the quality of, interferes with the performance of, or impairs the functionality of Plaintiff's computer systems, programs and networks; and
- j) Selling, publishing, distributing, or using any property or information obtained from Plaintiff's computer systems, programs and networks without Plaintiff's authorization;
- k) Removing, extracting, or copying any information or data from Plaintiff's computers systems, programs without Plaintiff's authorization;
- l) Awarding Plaintiff all costs and attorneys' fees to the full extent permitted under applicable law;
- m) Awarding Plaintiff pre- and post-judgment interest as permitted by law;
- n) Awarding any other relief as the Court may deem just and proper.

JURY DEMAND; Pursuant to Rule 38 of the Federal Rules of Civil Procedure,  
Plaintiff demands trial by jury in this action of all issues so triable.

Respectfully submitted in District of San Juan, Puerto Rico on this the 27th, day of  
August 2021.

Plaintiffs' Attorney,

S/*RAFAEL F. CASTRO LANG*  
RAFAEL F. CASTRO LANG  
Attorney for Appellant  
USDC-PR- 128505  
P O Box 9023222  
San Juan PR 00902-3222  
Tel: (787) 723-3672 - 723-1809  
Fax: (787) 725-4133  
Email: [rafacastrolang@gmail.com](mailto:rafacastrolang@gmail.com)  
[rafacastrolanglaw@gmail.com](mailto:rafacastrolanglaw@gmail.com)